Mobile Code Security Products - Enclave

DRAFT
Version 1.0

Date
September 19, 2000

Prepared By:
NSA
Booz-Allen & Hamilton
Litton TASC

Prepared For:
National Security Agency
(V43)

DISCLAIMER

Foreword

The National Security Agency (NSA) V43 Program Office requested the development of this protection profile to support the certification and accreditation of the Mobile Code Enclave. The Enclave one of the two area of focus for the Mobile Code effort.

The protection profile is a required part of the basis for certification and accreditation according to the NSA. The community of interest for this protection profile will be the developers, maintainers and certification authority of the V43.

Table Of Contents

List of Figures

List of Tables

Conventions and Terminology

Conventions

COMMON CRITERIA PRESENTATION CONVENTIONS

The notation, formatting, and conventions used in this protection profile (PP) are based on or consistent with version 2 of the Common Criteria (CC). Font style and clarifying information vehicle conventions were developed to aid the reader. Additionally, British English is used throughout the protection profile.

A font style convention was developed so that protection profiles will be consistent in the presentation of functional component operations. The family behaviour name is followed by the family short name in parentheses, and the short family name is superscripted following the requirement statement, e.g.:

> Audit Review (FAU_SAR.1)
>
> The TSF shall provide [an authorised administrator] with the capability to read [all trail data] from the audit records.FAU_SAR.1.1

The CC permits four functional component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. These operations are defined in Common Criteria, Part 2, paragraph 2.1.4 as

- assignment: allows the specification of an identified parameter;
- iteration: allows a component to be used more than once with varying operations;
- refinement: allows the addition of details; and
- selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicised, and underlined text. The author used brackets ("[]") to set off all assignments or selections that require future action by the developer. The text "assignment:" or "selection:" is indicated within the brackets. Iterations are set off with parentheses. The iteration "(#)" follows the short family name and "(iteration #)" follows the family behaviour.

Table 1-1 Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	The purpose of bolded text is used to alert the reader that additional text has been added to the CC. Example: The TSF shall export **(in ASCII format)** the **labeled** user data with the user data's associated security attributes.	Assignment Refinement

Convention	Purpose	Operation
Italics	The purpose of italicised text is to inform the reader of an appended assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [assignment: *list of additional SFP capabilities*].	Assignment Selection
Underline	The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to prevent modifications to the audit records.	Selection
Bold & Italics	The purpose of bolded and italicised text is to inform the reader that the author has added new text to the requirement and that an additional vendor action needs to be taken. Example: **Subject sensitivity label; Object sensitivity label; [assignment: *list of additional attributes that audit selectivity is based upon*].**	Assignment Refinement
Parentheses	The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times. Example: Basic data exchange confidentially (Iteration 1) FDP_UCT.1(1) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to transmit objects in a manner protected from unauthorised disclosure. FDP_UCT.1.1 Basic data exchange confidentially (Iteration 2) FDP_UCT.1(2) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to receive objects in a manner protected from unauthorised disclosure. FDP_UCT.1.1	Iteration

Convention	Purpose	Operation
Endnotes	The purpose of endnotes is to alert the reader that the author has deleted Common Criteria text. An endnote number is inserted at the end of the requirement, and the endnote is recorded on the last page of the section. The endnote statement first states that a deletion was performed and then provides the rationale. Following is the family behaviour or requirement in its original and modified form. A strikethrough is used to identify deleted text and bold for added text. A text deletion rationale is provided. Examples: Text as shown: **Guarantees of audit data availability** (FAU_SGT.1) [1] Endnote statement: A deletion of CC text was performed. Rationale: The component name was changed to …. ~~Protected audit trail storage~~ **Guarantees of audit data availability** (FAU_SGT.1) Text as shown: The TSF shall **be able to** prevent auditable events, except those taken by the authorised administrator, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1) [2] Endnote statement: A deletion of CC text was performed. Rationale: The words "with special rights" were deleted because …. The TSF shall **be able to** prevent auditable events, except those taken by the authorised administrator ~~with special rights~~, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1)	Refinement

Convention	Purpose	Operation
(EXP)	The purpose of using (EXP) after the family behaviour name is to alert the reader to and explicitly identify a newly created requirement. Example. **Object security attributes (EXP)** (FDP_OSA.1) **The TSF shall associate the following security attributes with named objects:** **a) Access control attributes, consisting of the following [assignment: *list of object attributes used to enforce the Discretionary Access Control Policy*.]** **b) Sensitivity label consisting of a hierarchical level and a set of non-hierarchical categories** **c) [Assignment: *other object security attributes*]. (EXP)** (FDP_OSA.1.1)	Refinement

As a means to provide the reader with additional requirement understanding or to clarify the author's intent, requirements overview and application notes are used.

The requirements overview are used to provide a discussion of the relationship between functional requirements so that the protection profile reader can understand why a component or group of components were chosen and what effect they are expected to have as a group of related functions. The requirements overview precedes either a component or a set of components.

To provide support information that is considered relevant or useful for the construction, evaluation, or use of the TOE, e.g., to clarify the intent of a requirement, to identify implementation choices, or to define "pass-fail" criteria for a requirement, application notes are used. Application notes follow the relevant requirement component.

NAMING CONVENTIONS

Explicit Requirements: The Common Criteria paradigm allows protection profile and security target authors to create their own requirements, termed explicit requirements, should the Common Criteria not offer suitable requirements to meet their needs. Explicit requirements must be identified and are required to use the Common Criteria class/family/component model in articulating these requirements. The naming convention for explicit requirements is the same as that used in the Common Criteria. There is a long name that is easily associated with the context of the requirement, and there is a short name, i.e., wxx_yyy.c.d, where w = F for function; A for assurance; xx = the class name; yyy = the component name; c = component; and d = element. To ensure these requirements are explicitly identified, the parenthetical phrase (EXP) is appended to the newly created short name. The newly created explicit requirements are

integrated with the CC requirements in alphabetical order by short name. The rationale for creating a requirement is provided in Section 6.6 Explicit Requirements Rationale.

Assumptions: TOE security environment assumptions are given names beginning with "A." and are presented in alphabetical order, e.g., A.ENCRYPT, A.NOPUBLIC.

Threats: TOE security environment threats are given names beginning with "T."and are presented in alphabetical order, e.g., T.ASPOOF, T.IMPORT .

Policies: TOE security environment policies are given names beginning with "P." and are presented in alphabetical order, e.g., P.NEED_TO_KNOW, P.TRAINING.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE." respectively and are presented in alphabetical order, e.g., O.AUDITING, O.RESIDUAL_INFORMATION, OE.BACKUP.

Terminology

The following list of commonly used terms is presented here to aid the reader:

Administrator	A defined role for the TOE or any person that has assumed that role.
Agent	Any authorised or unauthorised user.
Authorised User	A user who may, in accordance with the TSP, perform an operation.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	Members of a component; cannot be selected individually.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from CC, Part 3 that represents a point on the CC predefined assurance scale.
Object	An entity within the TOE Security Functions Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.
Package	A reusable set of either functional or assurance components (e.g., an EAL), combined together to satisfy a set of identified security objectives.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOE's that meet specific consumer needs.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Signed Mobile Code	Mobile Code bound with a PKI digital certificate. Signed Mobile code ensures code integrity and authenticity
Subject	An entity within the TSC that causes operations to be performed.
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TOE security policy.
Unauthorised User	Any person that is not authorised under the TOE security policy to access the TOE.

Document Organisation

Section 1 provides the introductory material for the protection profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next, Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

An acronym list is provided to define frequently used acronyms.

A reference section is provided to identify background material.

1— Introduction

The presence of executable content and mobile code has significantly increased in the computing environment. Executable content and mobile code is useful due to its ability to increase flexibility of applications, to meet various end user requirements, as a means of distributed computing, and is compatible with many platforms. Mobile code also raises serious security issues.

Related to mobile code is executable content. The difference between mobile code and executable content is that the former is derived from a network connection and the latter is not. The National Security Agency (NSA) has defined mobile code and executable content.

> Mobile Code is defined as text or data conveyed over a computer network, embedded in or referenced from other network data, and executed without explicit end-user initiation on the recipient platform.
>
> Executable Content is text or data embedded in or bound to documents or other data sets, and executed without explicit end-user initiation.

Mobile code technologies are very useful in extending and enabling sophisticated use of programs embedded in or bound to web pages, e-mail messages, word processor documents, and other content types. However, mobile code can also serve as a vehicle for security compromise.

Mobile code may be transferred to another user and executed with full access to local resources without the user's knowledge. Therefore, this mobile code may perform activities such as deletion, modification, or extraction of the user's data or degrade the performance of a system that could compromise the integrity or availability of a system. This code is called malicious mobile code.

The *Department of Defense (DoD) Mobile Code Technology Policy and Guidance* (DRAFT), *18 August 2000,* has derived an initial categorization of mobile code technologies. These categories are expected to be reviewed periodically and updated when necessary. Although this DoD document is still in draft, its intent is clear in providing a means of expressing various levels of risk into, currently, three categories.

> Category 1 mobile code technologies exhibit a broad functionality allowing unmediated access to host and remote systems and resources. Category 1 technologies have known security vulnerabilities with few or on countermeasures once access is gained (e.g., all or none decision: execute with full access to all system services or don't execute at all.) The following technologies are designated Category 1:
>
> ActiveX
> Windows Scripting Host, when used to execute mobile code
> Unix shell scripts
> Batch scripts

Category 2 mobile code technologies have full functionality allowing mediated access and environment-controlled access to host system services and resources. Category 2 technologies may have known security vulnerabilities but also have fine-grained, periodic, or continuous countermeasures or safeguards. The following technologies are designated Category 2:

Java applets and other Java mobile code
Visual Basic for Applications
LotusScript
PerfectScript
Postscript

Category 3 mobile code technologies supports limited functionality, with no capability for unmediated access to host system services and resources. Category 3 technologies may have a history of known vulnerabilities, but also support fine-grained, periodic, or continuous security safeguards. The following technologies are designated Category 3:

Javascript (include Jscript and ECMAScript variants)
VBScript
Portable Document Format
Shockwave/Flash

This protection profile focuses on the security requirements derived primarily from the needs of the DoD to provide a defense against malicious mobile code entering at the enclave boundary. This requirement is in alignment with the DoD Defense in Depth Strategy. However, threats and requirements defined in this profile are typical to the commercial sector and not unique to the DoD.

1.1 Identification

Title: Authors: Angus Forbes, Litton TASC; Paul Whitney, Booz*Allen&Hamilton; Neil Ziring, NSA V43; Craig Nedrow, Litton TASC; Bill VonHagel, Booz*Allen&Hamilton.

Vetting Status:

CC Version: 2.2 [ISO/IEC-15408]

General Status (e.g., active, superseded, retired)

Registration: MCESPPP;

NSA/Information System Security Organization

Keywords: Mobile Code Enclave

1.2 Protection Profile Overview

This Protection Profile specifies the National Security Agency V43 Program Office's requirements for security capabilities to support the Mobile Code efforts. The Mobile Code: Enclave represents a component of the Mobile Code effort as defined in Section 1.0 Introduction. The Target of Evaluation (TOE) is the Enclave. The Protection Profile defines the threats to the information systems of the Enclave Systems, defines implementation-independent security objectives of the TOE and its environment, defines the functional and assurance requirements, and provides the rationale for the security objectives.

1.3 Related Protection Profiles

Definitions and overall introductions outline were derived simultaneously with the Mobile Code: Desktop Protection Profile (MCDSPPP). All of the authors of this PP were also a contributor to the Mobile Code: Desktop.

2— TOE Description

The target of evaluation (TOE) is malicious mobile code detection and mitigation systems. Specifically, it is the mobile code detection and mitigation system that would be placed on the boundary of an enclave, so as to protect the enclave from mobile code threats from external networks.

Mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, embedded in or referenced from other network data, and executed on a local system without explicit installation or execution by the recipient.

Malicious mobile code is software designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources.

Although the use of email to transfer executable code might be considered a type of mobile code, it presents specialized challenges. As such, separate products may be needed to mitigate email-based mobile code. Therefore, email will not be explicitly addressed in this protection profile.

Figure 1 shows the TOE Environment. Sites on the Internet or other networks external to the enclave may have mobile code that can be downloaded by a user within the enclave. An enclave has a defined boundary, usually subject to a boundary security policy enforced by a firewall or other security product. The mobile code protection and mitigation system will be located at the enclave boundary or inside the enclave. The user host inside the enclave will be configured to access external resources through the TOE.

The TOE boundary is shown in Figure 1 as the shaded block. The TOE functionality may be composed of a standalone device or devices, or may reside on another device such as a firewall. The TOE may scan all incoming data, or it may get a subset of data vectored to it via another device such as a firewall. All data received by the TOE will be scanned.

The malicious mobile code protection and mitigation system will be capable of protecting the enclave by enforcing security policy rules set by an enclave administrator. Once it detects malicious mobile code, it will alert the administrator, create an audit log of the event, and take one or more of several actions:

- Delete or quarantine the offending code.
- Set an alarm and send the code through to the enclave
- Modify the code and send it through to the enclave
- Stop the code from proceeding into the enclave

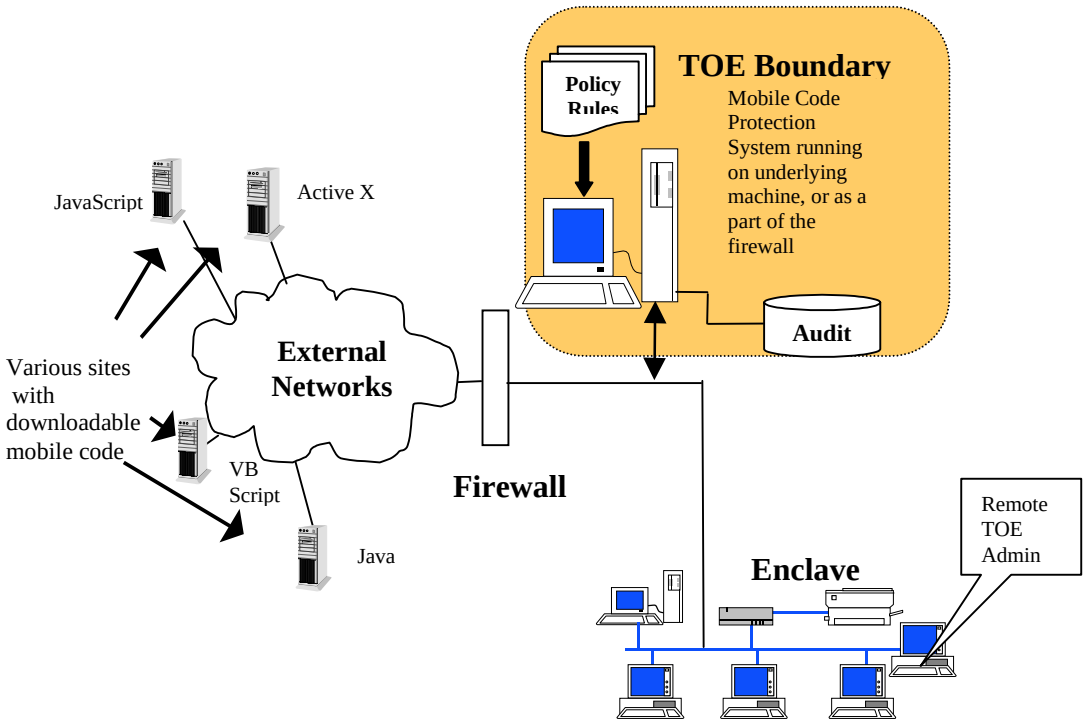

Figure 1: TOE Environment – Malicious Mobile Code

The types of mobile code that are potential threats are large and growing. Types of mobile code that the TOE must be able to detect and filter are listed below.

- ActiveX
- Java
- JavaScript
- VBScript

Mobile Code types listed above are mandatory, but TOE implementations may specify additional mobile code types in their security targets.

Products based upon this profile are intended to assist the enclave in complying with the Department of Defense (DoD) Mobile Code policy. This policy defines different categories of Mobile Code. Each category specifies a different level of access to client system resources. The TOE must be configurable such that different subsets of end users may be able to receive different types or categories of mobile code.

The malicious code detection and mitigation software will address several Application Layer (OSI Layer 7) protocols. These will include FTP and HTTP, as a minimum.

The TOE will have its own administrative domain. It will apply its own identification and authorization mechanisms to allow access to administration capabilities, which are in addition to those provided by the host operating system. Enclave users will not be able to have access to the TOE administrative capabilities. The TOE can be administered either from within the TOE boundary or from within the enclave.

The TOE will support the capability for the administrator to configure the security policies of the malicious mobile code protection system.

The TOE will have auditing/logging/alerting functions. The audit log is a responsibility of the malicious mobile code detection and mitigation software. Requirements for the audit log are:

- Record auditable events
- Record violations of policies
- Alert administrators to potential security violations.

3— TOE Security Environment

The purpose of the TOE Security Environment section is to define the nature and scope of the security needs to be addressed by the TOE. This section will involve a discussion of:

a. Any assumptions that are made regarding the TOE security environment, thereby defining the scope of the security needs;

b. The assets requiring protection (typically information or resources within the IT environment or the TOE itself), the identified threat agents, and the threats they pose to the assets;

c. The organisational security policies or rules with which the TOE must comply in addressing the security needs.

Subsequent sections of the PP and ST show how the security needs will be addressed by the TOE, in combination with its operating environment.

In this section, the terms “enclave user” and “user” refer to individuals authorized to access resources inside the enclave and authorized to employ the services of the TOE for access to data and mobile code outside the enclave. The term “administrator” and “TOE administrator” refer to individuals authorized to administer the TOE and responsible for configuring and maintaining the TSF. The term “authorized personnel” refers to all users and administrators.

3.1 Secure Usage Assumptions

This section discusses the scope of intended usage of the TOE as well as assumptions about the operating environment including physical, personnel, and connectivity issues.

A.DESIGN The design, manufacturing and delivery of the TOE will operate within specification limits and will comply with security requirements.

A.ENCLAVE_INTEGRITY The communication between the TOE and the users operates within a controlled access environment that provides protection against unauthorised access and modification that is consistent with the sensitivity of the traffic that it is filtering. This assumption will also include the channels over which TOE administered.

A.ENVIRONMENT The TOE operates within a controlled access environment that provides protection against unauthorised physical access and tampering that is consistent with the sensitivity of the information contained therein.

A.NO_EVIL The TOE administrator will not actively compromise or degrade the TSP.

A.SECURE The TOE will operate in an accredited system configuration and all system resources (hardware, software, firmware) will operate in that configuration. (Note: The term “accredited” as used refers to the certification process established by NAIP Labs.)

A.TRAIN	All authorised personnel will be trained on the proper operation and procedures of the TOE.
A.USER_TRANSPARENT	Application of the TSF to user traffic is transparent to the users.

3.2 Threats to Security

The TOE will provide protection against the threats defined below. The determination of adequate threat mitigation is addressed in Section 6, Rationale.

The attacks associated with the following threats may be motivated by deliberate malice or could be the result of unintentional mistakes on behalf of the information systems due to the attacker's advantage of knowing the system configuration and thus its vulnerabilities.

The threats listed below are those that are addressed by the TOE that is compliant with this Protection Profile. The term "compromise" (when unqualified) refers to a degradation of the confidentiality, availability, and/or integrity of an asset.

Projected Threat Environment: Mobile Code Enclave components will be vulnerable to the same physical threat as the units with which it will be deployed. Therefore, threat agents are assumed to have a high degree of motivation, sufficient resources, and expertise to mount significant information warfare attacks against the Mobile Code Enclave System. Information systems and networks are vulnerable to numerous threats including:

T.ACCESS	An unauthorised individual gains access to the TOE administrative functions by utilising vendor proprietary maintenance mechanisms and/or pre-established user accounts.
T.ALTER	An unauthorised individual may surreptitiously gain access to the TOE and attempt to alter and/or replace system elements (e.g., hardware, firmware, or software and data) and thereby compromise the TOE.
T.AUDFAIL	System modification, compromise, or audit file "full" may result in failure to collect audit data.
T.AUDREV	Appropriate individuals may fail to adequately review and interpret audit data or take appropriate action.
T.BACKUP	Failure to adequately perform system backup of TOE Security Function (TSF) data may result in compromise or non-availability of the TOE.
T.DENIAL	An unauthorised administrator may render the TOE systems unavailable for use.

T.ERROR	An authorised administrator performs erroneous actions that will compromise user and/or system resources.
T.IMPERSONATE	An unauthorised individual may attempt to gain access to the TOE by pretending to be an authorised administrator.
T.IMPLEMENT	Due to the implementation process, the TOE may have intentional or unintentional errors that may allow unauthorised access.
T.IMPORT	Malicious code may be introduced into the system, resulting in a compromise of the integrity and/or availability of the TOE.
T.INTRUDE	An unauthorised individual may gain access to one or more components of the TOE or the TOE network from an outside network.
T.MEDIA	Failure to adequately protect storage media may result in compromise or non-availability of the TOE.
T.PHYSICAL	Security-critical parts of the TOE may be subject to physical attack or enemy capture that may compromise security.
T.REPEAT	An unauthorised individual may repeatedly attempt to guess authentication information.
T.TRAFFIC	Use of the TOE may unintentionally transmit sensitive information to unauthorised users.
T.TRAIN	Insufficient user training on TOE security features may result in system vulnerabilities.
T.VIRUS	An authorised administrator may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of the TOE.

3.3 Organisational Security Policies

The TOE must provide protection under the policies defined below. The organisational security policies define the operation, management, personnel responsibilities and guidelines that must be enforced to provide security for the TOE. A number of documents were referenced to obtain the relevant policies that apply to the TOE. The following policy statements are derived from the following references:

- *Department of Defense (DoD) Mobile Code Technology Policy and Guidance, (DRAFT) 18 August 2000.*

- *Definition and Risk Categorization for Mobile Code Formats, Version 1.0, 12 November 1999*

Organisational security policies support objectives that are presented in Section 4 – Security Objectives of this protection profile. A single security objective may be supported by multiple security policies. Security policies are organisational guidelines and practices that support the security objectives for the TOE.

P.ACCOUNTABLITY User activity will be monitored to the extent that audit and system controls are applied properly to users, administrators and system processes.
Accountability – NSTISSI 4009 defines accountability as an "(IS) Property allowing auditing of IS activities to be traced to persons or processes that may then be held responsible for their actions".
Accountability – DITSCAP follows NSTISSI 4009 but includes:
*Authenticity – (DITSCAP) The property that allows the ability to validate the claimed identity of a system entity.
*Non-Repudiation – NSTISSI 4009 defines non-repudiation as "Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data".

P.AVAILABILITY The TOE will provide timely, reliable access to information and system resources to meet operational requirements.
NSTISSI 4009/DITSCAP defines Availability as "timely, reliable access to data and information services for authorized users".

P.CONFIDENTIALITY The TOE will provide security features assuring that information is not disclosed to unauthorised persons, processes, or devices.
NSTISSI 4009/DITSCAP defines Confidentiality as "Assurance that information is not disclosed to unauthorized persons, processes, or devices". The focus of confidentiality is national security-relevant information. P.CONFIDENTIALITY must be applied *at all times*—there are no exceptions.

P.CONFIGURABILITY The TOE will provide configurations of allowable policies of the TOE definable at the system or user levels.

P.DATA The network and host on which the TOE is installed will be configured to route all applicable data through the TOE to ensure that the TSP will be met.

P.FILTER Once the TOE detects malicious code, the TOE will apply remediative measures in accordance with the TSP.

P.INTEGRITY	The TOE will provide controls to protect the integrity of information and system resources, including maintaining the integrity of the TSF in the event of a system failure (e.g., fail-safe). NSTISSI 4009/DITSCAP defines integrity as “Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.”
P.INTERFACE	The TOE shall apply its TSP to all interfaces.
P.MANAGE	The TOE will be managed such that the TSFs are properly activated, implemented and preserved throughout its operational lifetime.
P.PORT	Administrators of the TOE will not export/import TSF data without proper and explicit authorisation.
P.TRAINING	All TOE administrators will be properly trained on the TSF prior to accessing an operational TOE.

4— Security Objectives

4.1 Security Objectives for the TOE

This section defines the security objectives of the TSF and its supporting environment. Security objectives reflect the stated intent to counter identified threats and/or comply with any organisational security policies identified. All of the identified threats and organisational policies are addressed under this section or under section 4.2.

O.ACCESS_ADMIN	Administrators access can be either from within the TOE or within enclave.
O.ACCESS_USER	The TOE will be configured such that all users within the enclave will be subject to the policy of the TSP.
O.ALL_DATA	The TOE will scan all data received. (See Section 2 "TOE Description")
O.AUDIT	The TOE will provide means of recording any security relevant events, so as to assist an administrator in detection of potential attacks or mis-configuration of the TOE security features that would leave the network susceptible to attack, and also hold administrators accountable for any actions they perform that are relevant to security.
O.DETECT	The TOE will detect and mitigate malicious mobile code.
O.I&A	Security components and critical network components will be protected by strong identification and authentication mechanisms. These mechanisms will identify all administrators and will authenticate the claimed identity before granting an administrator access to the TOE network.
O.INTERFACE	The TOE must support the capability to interface with gateways connected to external networks and internal enclave networks. (REMOTE USERS)
O.POLICY	The TOE will support both administrative access policies and malicious mobile code policies.
O.PROTECT	The TOE will ensure the protection of its TSP and storage. This protection will include the following: 1) Fail Safe capability 2) Secure initialization in the event of unplanned power outage
O.SELF_PROTECT	The TOE will provide a means to protect itself from automated malicious mobile code by blocking the code and alert the administrator

for immediate action. The TOE will also have a capability to update itself against new malicious mobile code threats.

4.2 Security Objectives for the Environment

This section defines the security objectives of the supporting environment of the TSF. Security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified.

A Mobile Code Enclave-conformant TOE is not assumed to be complete and self-contained and, as such, is dependent upon other Mobil Code subsystems. Certain objectives with respect to the general operating environment must be met. The following are the Mobile Code Enclave security objectives for the environment.

OE.ADMIN	The administrator will plan, configure, audit, and manage policies at the system and user levels.
OE.AUDITLOG	Administrators of the TOE must ensure audit facilities are used and managed effectively.
OE.BACKUP	Periodic backups will be performed to protect security-critical TOE resources.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed and operated in a manner which maintains the system security.
OE.PHYSICAL	Those responsible for the TOE must ensure that any parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.
OE.TRAIN	Authorised administrators must be trained on the proper operation of TOE security functions. Additionally, TOE security parameters are established by administrators according to security policies and practices.

5— IT Security Requirements

5.1 TOE Security Functional Requirements

The unique nature of the TOE creates interpretation problems for traditional information technology and information security terminology. The Common Criteria defines security requirements for information technology and security without regards to unusual IT environments. The nature of this document is to define an "implementation independent" set of requirements to address information security features and controls.

Terminology such as "session", "login", or "user accounts" is intended to convey traditional methods of discreet computer processing sessions, individual identification and authentication and access control features. The ST writer may choose to implement or recommend different terminology to describe equivalent concepts. This is permissible provided the ST writer describes the intent of each term and the corresponding impact on information security.

Terminology such as "user data" is intended to identify any data or information that is transmitted, processed or stored by the TOE that is not specifically TSF (TOE Security Function) related.

5.1.1 Security Audit (FAU)

5.1.1.1 Security alarms (FAU_ARP.1)

The TSF shall take [*assignment: add a record to the audit log, alert the administrator if so indicated by the TSP*] upon detection of a potential security violation. FAU_ARP.1.1

5.1.1.2 Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *not specified*] level of audit; and

c) [*assignment: client request, detection of mobile code in response data, application of any change to response data*]. FAU_GEN.1.1

The TSF shall record within each audit record at least the following information:

(Application Note: With respect to FAU_GEN.1.1 the TOE must be able to log both phases of a transaction with an external resource: the request and the response. These may be in the same audit log record or separate ones.)

d) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

e) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *address or host name of client, request identification or URL, type of mobile code detected (if any), change applied to response data (if any)*] FAU_GEN.1.2

(Application Note: If the TOE takes remediative action which involves deleting or modifying data from an external resource then the form of that action must be logged.)

5.1.1.3 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_GEN.2.1

(Application Note: there are two kinds of users: enclave users and administrators. Administrators shall be identified by name in audit records, enclave users may be identified by information specified in the Security Target, which must include either a user name, a host name, or an IP address of an enclave host.)

5.1.1.4 Potential violation analysis (FAU_SAA.1)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP FAU_SAA.1.1

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination *of* [assignment: s*ubset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*]. FAU_SAA.1.2

(Application Note: ST writer is responsible for the assignments on the above functional requirement for this TOE implementation. At a minimum, the TOE must be able to maintain a list of external sources that have supplied data found to violate the TSP.)

5.1.1.5 Audit review (FAU_SAR.1)

The TSF shall provide [assignment: *administrators*] with the capability to read [assignment: *all information*] from the audit records. FAU_SAR.1.1

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

5.1.1.6 Restricted audit review (FAU_SAR.2)

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

(Application Note: Only administrators are authorised to read audit logs because the information in them may be sensitive. Support to this requirement is essential for the TOE to support P.CONFIDENTIALITY.)

5.1.1.7 Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [selection: *subject identity, host identity, event type*]

b) [assignment: *time interval*]. FAU_SEL.1.1

5.1.1.8 Protected audit trail storage (FAU_STG.1)

The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.1.1

The TSF shall be able to [selection: *prevent*] modifications to the audit records. FAU_STG.1.2

5.1.1.9 Action in case of possible audit data loss (FAU_STG.3)

The TSF shall take [assignment: *roll over the audit log or cease providing service*] if the audit trail exceeds [assignment: *available storage or an administrator-configured fixed size limit*]. FAU_STG.3.1

5.1.2 Cryptographic Support (FCS)

5.1.2.1 Cryptographic key access (FCS_CKM.3)

The TSF shall perform [assignment: *public key retrieval*] in accordance with a specified cryptographic key access method [assignment: *by extracting the key from a validated public key certificate*] that meets the following: [assignment: X.509 (any version, including at a minimum, X.509 version 3)]. FCS_CKM.3.1

5.1.2.2 Cryptographic operation (FCS_COP.1)

The TSF shall perform [assignment: *signature validation*] in accordance with a specified cryptographic algorithm [assignment: *RSA or DSA*] and cryptographic key sizes [assignment: *512 bits or larger*] that meet the following: [assignment: *RSA PKCS #1 or the NIST Digital Signature Standard (FIPS-FIPS PUB 186-2*]. FCS_COP.1.1

(Application Note: This requirement is intended to support validation of signed mobile code by the TOE. Performing signature validation on mobile code requires use of validated certificates. Mechanisms for validation of certificates are left to the ST writers,

but must be specified. The designation of validated certificates may be done by the administrators.)

5.1.3 User Data Protection (FDP)

5.1.3.1 Complete access control (FDP_ACC.2)

The TSF shall enforce the [assignment: *assigned URL access list, if any*] on [assignment: *all network access requests*] and all operations among subjects and objects covered by the SFP. FDP_ACC.2.1

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

(Application Note: The URL access list included in the SFP must specify external resources to a host or IP address granularity at a minimum. The access list may be positive (permitted external sources) or negative (prohibited external sources) or both.)

5.1.3.2 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the [assignment: *assigned mobile code access restrictions*] to objects based on [assignment: *mobile code type, URL of external source, signature verification status, and identity of client user*]. FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *as specified in target*]. FDP_ACF.1.2

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *specific identification of 'allowed' sources by the administrator*]. FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on the [assignment: *specific identification of 'prohibited' sources by the administrator*]. FDP_ACF.1.4

5.1.3.3 Complete information flow control (FDP_IFC.2)

The TSF shall enforce the [assignment: *mobile code access policy rules*] on [assignment: *all client users*] and all operations that cause that information to flow to and from subjects covered by the SFP. FDP_IFC.2.1

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. FDP_IFC.2.2

5.1.3.4 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the [assignment: *mobile code access policy rules*] based on the following types of subject and information security attributes: [assignment: *mobile code access policy rules: type of mobile code, identity of external source, identity of requesting client user, and any additional aspects of the mobile code data itself, as specified in target*]. FDP_IFF.1.1

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for accessing mobile code, the source must be permitted, and the mobile code type must be permitted, and the client user must be authorized access to that type of mobile code*]. FDP_IFF.1.2

The TSF shall enforce the [assignment: *as specified in target*]. FDP_IFF.1. 3

The TSF shall provide the following [assignment: *the TOE must be able to recognize and correctly identify at least the following mobile code types: Javascript, VBScript, Java, ActiveX; embedded in HTML, regardless of whether that HTML is syntactically correct as parsed against its claimed DTD*]. FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *as specified in target*]. FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *as specified in security target*]. FDP_IFF.1.6

5.1.3.5 Import of user data without security attributes (FDP_ITC.1)

The TSF shall enforce the [assignment: *mobile code access restrictions*] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.1.1

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. FDP_ITC.1.2

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules as specified in target*]. FDP_ITC.1.3

(Application Note: This requirement applies to mobile code that is not digitally signed.)

5.1.3.6 Import of user data with security attributes (FDP_ITC.2)

The TSF shall enforce the [assignment: *mobile code access restrictions*] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.1

The TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.2

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.3

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. FDP_ITC.2.4

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: signed mobile code for which signature verification fails shall be immediately deleted by the TOE, and shall not be transmitted to the user]. FDP_ITC.2.5

(Application Note: This requirement applies to mobile code that is digitally signed.

5.1.3.7 Full residual information protection (FDP_RIP.2)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *deallocation of the resource from*] all objects. FDP_RIP.2.1

(Application Note: This requirement also applies to caching of external data by the TOE if the TOE implementation supports caching.)

5.1.4 Identification and Authentication (FIA)

(Application Note: All I&A functions dealing with this family only applies to TOE administrative users.)

5.1.4.1 Authentication failure handling (FIA_AFL.1)

The TSF shall detect when [assignment: *as specified in target*] unsuccessful authentication attempts occur related to [*assignment: administrator login*]. FIA_AFL.1.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions as specify in target*]. FIA_AFL.1.2

5.1.4.2 User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *administrative rights*]. FIA_ATD.1.1

5.1.4.3 Verification of secrets (FIA_SOS.1)

The TSF shall provide a mechanism to verify that secrets meet [assignment: *an administrator-assigned minimum password length*]. FIA_SOS.1.1

5.1.4.4 Timing of authentication (FIA_UAU.1)

The TSF shall allow [assignment: *selection or specification of an administrator identity*] on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.1.2

5.1.4.5 Protected authentication feedback (FIA_UAU.7)

The TSF shall provide only [assignment: *in progress announcement*] to the user while the authentication is in progress. FIA_UAU.7.1

5.1.4.6 Timing of identification (FIA_UID.1)

The TSF shall allow [assignment: *none*] on behalf of the user to be performed before the user is identified. FIA_UID.1.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.1.2

(Application Note: The TOE administrator must identify themselves before performing any administrative actions or affecting the TSP in any way.)

5.1.4.7 User-subject binding (FIA_USB.1)

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. FIA_USB.1.1

5.1.5 Security Management (FMT)

5.1.5.1 Management of security functions behaviour (FMT_MOF.1)

The TSF shall restrict the ability to [selection: *enable, add, delete, or modify*] the functions [assignment: *mobile code security policy rules*] to [assignment: *administrators*]. FMT_MOF.1.1

5.1.5.2 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the [assignment: *access control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *add, delete, or modify*] the security attributes [assignment: *specific client user privileges*] to [assignment: *administrators*]. FMT_MSA.1.1

5.1.5.3 Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes. FMT_MSA.2.1

5.1.5.4 Static attribute initialisation (FMT_MSA.3)

The TSF shall enforce the [assignment: *information flow SFP*] to provide [selection: *uniform restrictive*] default values for security attributes that are used to enforce the *SFP*. FMT_MSA.3.1

(Application Note: Uniform restrictive is meant that the TOE will supply the same default values for security attributes for all client users.)

The TSF shall allow the [assignment: *administrator*] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.5.5 Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to [selection: *modify, delete, add* [assignment: *administrator privileges, auditable events, audit log format, audit log location, user client rights, mobile code access restrictions, mobile code remediation resources, permitted remote administration hosts (if any), additional as specified in security target*] the [assignment: *administrators*] to [assignment: the authorised identified roles]. FMT_MTD.1.1

5.1.5.6 Revocation (FMT_REV.1)

The TSF shall restrict the ability to revoke security attributes associated with the [selection: *client users, administrators, public key certificates, types of mobile code*] within the TSC to [assignment: *administrators*]. FMT_REV.1.1

The TSF shall enforce the rules [assignment: *all revocations will be recorded in the audit log*]. FMT_REV.1.2

5.1.5.7 Security roles (FMT_SMR.1)

The FMT_SMR.1TSF shall maintain the roles [assignment: *administrator*]. FMT_SMR.1.1

The TSF shall be able to associate users with roles. FMT_SMR.1.2

5.1.6 Protection of TOE Security Functions (FPT)

5.1.6.1 Abstract machine testing (FPT_AMT.1)

The TSF shall run a suite of tests [selection: *during initial start-up*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.1.6.2 Failure with preservation of secure state (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur: [assignment: *power failure, operating system crash*]. FPT_FLS.1.1

5.1.6.3 Inter-TSF availability within a defined availability metric (FPT_ITA.1)

The TSF shall ensure the availability of [assignment: *mobile code security policy rules, audit log*] provided to a remote trusted IT product within [assignment: *as specified in target*] given the following conditions [assignment: *specified by the administrator*]. FPT_ITA.1.1

5.1.6.4 Automated recovery (FPT_RCV.2)

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.1

For [assignment: administrator-requested restart, orderly host shutdown and reboot], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.2.2

5.1.6.5 Non-bypassability of the TSP (FPT_RVM.1)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.1.6.6 TSF domain separation (FPT_SEP.1)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1

The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2

5.1.6.7 Reliable time stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.1.6.8 Inter-TSF basic TSF data consistency (FPT_TDC.1)

The TSF shall provide the capability to consistently interpret [assignment: *public key certificates*] when shared between the TSF and another trusted IT product. FPT_TDC.1.1

The TSF shall use [assignment: *X.509 any version, at a minimum X.509.3*] when interpreting the TSF data from another trusted IT product. FPT_TDC.1.2

(Application Note: This requirement applies to case where the TOE as the ability to obtain certificates from remote trusted repositories, such as directory services.)

5.1.6.9 TSF testing (FPT_TST.1)

The TSF shall run a suite of self tests [selection: *during initial start-up* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF. FPT_TST.1.1

The TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

5.1.7 TOE Access (FTA)

5.1.7.1 Limitation on scope of selectable attributes (FTA_LSA.1)

The TSF shall restrict the scope of the session security attributes [assignment: *as specified in security target*], based on [assignment: *identity of client user or host, and additional as specified in security target*]. FTA_LSA.1.1

5.1.7.2 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. FTA_MCS.1.1

The TSF shall enforce, by default, a limit of [assignment: *as specified in target*] sessions per user. FTA_MCS.1.2

5.1.7.3 TSF-initiated termination (FTA_SSL.3)

The TSF shall terminate an interactive session after a [assignment: *as specified in target*]. FTA_SSL.3.1

5.1.7.4 TOE session establishment (FTA_TSE.1)

The TSF shall be able to deny session establishment based on [assignment: identity of client host, and additional as specified in security target]. FTA_TSE.1.1

5.1.8 Trusted Path/Channels

5.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. FTP_ITC.1.1

The TSF shall permit [selection: *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel. FTP_ITC.1.2

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*]. FTP_ITC.1.3

5.1.8.2 Trusted path (FTP_TRP.1)

The TSF shall provide a communication path between itself and [selection: *remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. FTP_TRP.1.1

The TSF shall permit [selection: *remote administrator users*] to initiate communication via the trusted path. FTP_TRP.1.2

The TSF shall require the use of the trusted path for [*selection: all administrative functions*, [assignment: *as specified in target*]]. FTP_TRP.1.3

5.2 TOE Security Assurance Requirements

This protection profile specifies a minimum evaluated assurance level (EAL) for all security-critical IT components within the Mobile Code Enclave. This minimum level is EAL 2 (augmented). The Security Target (ST) author should specify the following in the TOE Summary Specification section of the ST:

- the overall TOE security architecture,
- the security-critical IT components within the architecture,
- the proposed EAL for each security-critical IT component (EAL 2 minimum).

The assurance requirements are taken from Part 3 of the CC. The details of assurance requirements are listed only once; however, Application Notes for each independent partition are listed separately.

EAL 2 is summarised in the following table. The following requirements have been augmented to those mandated by EAL 2:

- Systematic flaw remediation (ALC_FLR.1)

And Maintenance of Assurance requirements:

- Assurance maintenance plan (AMA_AMP.1)
- TOE component categorization report (AMA_CAT.1)
- Evidence of assurance maintenance (AMA_EVD.1)
- Security impact analysis (AMA_SIA.1)

Table 5-1 Assurance Requirements for the TOE: EAL 2

Assurance Class	Assurance Components
Configuration Management	Configuration items ACM_CAP.2
Delivery and Operations	Delivery procedures ADO_DEL.1 Installation, generation, and start-up procedures ADO_IGS.1

Assurance Class	Assurance Components
Development	Informal functional specification ADV_FSP.1 Descriptive high-level design ADV_HLD.1 Informal correspondence demonstration ADV_RCR.1
Guidance documents	Administrator guidance AGD_ADM.1 User guidance AGD_USR.1
Life Cycle Support	Flaw Remediation ALC_FLR.1
Tests	Evidence of coverage ATE_COV.1 Functional testing ATE_FUN.1 Independent testing – sample ATE_IND.2
Vulnerability Assessment	Strength of TOE security function evaluation AVA_SOF.1 Developer vulnerability analysis AVA_VLA.1
Maintenance of Assurance	Assurance Maintenance Plan AMA_AMP.1 TOE Component Categorisation Report AMA_CAT.1 Evidence of Assurance Maintenance AMA_EVD.1 Security Impact Analysis AMA_SIA.1

Configuration items (ACM_CAP.2)

The developer shall provide a reference for the TOE. ACM_CAP.2.1D

The developer shall use a CM system. ACM_CAP.2.2D

The developer shall provide CM documentation. ACM_CAP.2.3D

The reference for the TOE shall be unique to each version of the TOE. ACM_CAP.2.1C

The TOE shall be labelled with its reference. ACM_CAP.2.2C

The CM documentation shall include a configuration list. ACM_CAP.2.3C

The configuration list shall describe the configuration items that comprise the TOE. ACM_CAP.2.4C

The CM documentation shall describe the method used to uniquely identify the configuration items. ACM_CAP.2.5C

The CM system shall uniquely identify all configuration items. ACM_CAP.2.6C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ACM_CAP.2.1E

Delivery procedures (ADO_DEL.1)

The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.1.1D

The developer shall use the delivery procedures. ADO_DEL.1.2D

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. ADO_DEL.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADO_DEL.1.1E

Installation, generation, and start-up procedures (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. ADO_IGS.1.1D

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. ADO_IGS.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADO_IGS.1.1E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration. ADO_IGS.1.2E

Informal functional specification (ADV_FSP.1)

The developer shall provide a functional specification. ADV_FSP.1.1D

The functional specification shall describe the TSF and its external interfaces using an informal style. ADV_FSP.1.1C

The functional specification shall be internally consistent. ADV_FSP.1.2C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. ADV_FSP.1.3C

The functional specification shall completely represent the TSF. ADV_FSP.1.4C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_FSP.1.1E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements. ADV_FSP.1.2E

Descriptive high-level design (ADV_HLD.1)

The developer shall provide the high-level design of the TSF. ADV_HLD.1.1D

The presentation of the high-level design shall be informal. ADV_HLD.1.1C

The high-level design shall be internally consistent. ADV_HLD.1.2C

The high-level design shall describe the structure of the TSF in terms of subsystems. ADV_HLD.1.3C

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ADV_HLD.1.4C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. ADV_HLD.1.5C

The high-level design shall identify all interfaces to the subsystems of the TSF. ADV_HLD.1.6C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ADV_HLD.1.7C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_HLD.1.1E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements. ADV_HLD.1.2E

Informal correspondence demonstration (ADV_RCR.1)

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ADV_RCR.1.1D

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF

representation is correctly and completely refined in the less abstract TSF representation. ADV_RCR.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_RCR.1.1E

Administrator guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel. AGD_ADM.1.1D

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. AGD_ADM.1.1C

The administrator guidance shall describe how to administer the TOE in a secure manner. AGD_ADM.1.2C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. AGD_ADM.1.3C

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE. AGD_ADM.1.4C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. AGD_ADM.1.5C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. AGD_ADM.1.6C

The administrator guidance shall be consistent with all other documentation supplied for evaluation. AGD_ADM.1.7C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. AGD_ADM.1.8C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AGD_ADM.1.1E

User guidance (AGD_USR.1)

The developer shall provide user guidance. AGD_USR.1.1D

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The user guidance shall describe the use of user-accessible security functions provided by the TOE. AGD_USR.1.2C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. AGD_USR.1.3C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. AGD_USR.1.4C

The user guidance shall be consistent with all other documentation supplied for evaluation. AGD_USR.1.5C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. AGD_USR.1.6C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AGD_USR.1.1E

Systematic flaw remediation (ALC_FLR.1)

The developer shall document the flaw remediation procedures. ALC_FLR.1.1D

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. ALC_FLR.1.1C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.1.2C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. ALC_FLR.1.3C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. ALC_FLR..1.4C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ALC_FLR.1.1E

Evidence of coverage (ATE_COV.1)

The developer shall provide evidence of the test coverage. ATE_COV.1.1D

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ATE_COV.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_COV.1.1E

Functional testing (ATE_FUN.1)

The developer shall test the TSF and document the results. ATE_FUN.1.1D

The developer shall provide test documentation. ATE_FUN.1.2D

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ATE_FUN.1.1C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. ATE_FUN.1.2C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ATE_FUN.1.5C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_FUN.1.1E

Independent testing - sample (ATE_IND.2)

The developer shall provide the TOE for testing. ATE_IND.2.1D

The TOE shall be suitable for testing. ATE_IND.2.1C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_IND.2.1E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified. ATE_IND.2.2E

The evaluator shall execute a sample of tests in the test documentation to verify the developer's test results. ATE_IND.2.3E

Strength of TOE security function evaluation (AVA_SOF.1)

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. AVA_SOF.1.1D

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. AVA_SOF.1.1C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ ST. AVA_SOF.1.2C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AVA_SOF.1.1E

The evaluator shall confirm that the strength claims are correct. AVA_SOF.1.2

Developer vulnerability analysis (AVA_VLA.1)

The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP. AVA_VLA.1.1D

The developer shall document the disposition of obvious vulnerabilities. AVA_VLA.1.2D

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. AVA_VLA.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AVA_VLA.1.1E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed. AVA_VLA.1.2E

Assurance maintenance plan (AMA_AMP.1)

The developer shall provide an AM Plan. AMA_AMP.1.1D

The AM Plan shall contain or reference a brief description of the TOE, including the security functionality it provides. AMA_AMP.1.1C

The AM Plan shall identify the certified version of the TOE, and shall reference the evaluation results. AMA_AMP.1.2C

The AM Plan shall reference the TOE component categorization report for the certified version of the TOE. AMA_AMP.1.3C

The AM Plan shall define the scope of changes to the TOE that are covered by the plan. AMA_AMP.1.4C

The AM Plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact. AMA_AMP.1.5C

The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE. AMA_AMP.1.6C

The AM Plan shall identify the individual(s) who will assume the role of developer security analyst for the TOE. AMA_AMP.1.7C

The AM Plan shall describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed. AMA_AMP.1.8C

The AM Plan shall describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly. AMA_AMP.1.9C

The AM Plan shall justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE. AMA_AMP.1.10C

The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation. AMA_AMP.1.11C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AMA_AMP.1.1E

The evaluator shall confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with the proposed changes to the TOE. AMA_AMP.1.2E

TOE component categorization report (AMA_CAT.1)

The developer shall provide a TOE component categorization report for the certified version of the TOE. AMA_CAT.1.1D

The TOE component categorization report shall categorize each component of the TOE, identifiable in each TSF representation from the most abstract to the least abstract, according to its relevance to security; as a minimum, TOE components must be categorized as one of TSP-enforcing or non-TSP-enforcing. AMA_CAT.1.1C

The TOE component categorization report shall describe the categorization scheme used, so that it can be determined how to categorize new components introduced into the TOE, and also when to re-categorize existing TOE components following changes to the TOE or its security target. AMA_CAT.1.2C

The TOE component categorization report shall identify any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target. AMA_CAT.1.3C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AMA_CAT.1.1E

The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version. AMA_CAT.1.2E

Evidence of assurance maintenance (AMA_EVD.1)

The developer security analyst shall provide AM documentation for the current version of the TOE. AMA_EVD.1.1D

The AM documentation shall include a configuration list and a list of identified vulnerabilities in the TOE. AMA_EVD.1.1C

The configuration list shall describe the configuration items that comprise the current version of the TOE. AMA_EVD.1.2C

The AM documentation shall provide evidence that the procedures documented or referenced in the AM Plan are being followed. AMA_EVD.1.3C

The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE. AMA_EVD.1.4C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AMA_EVD.1.1E

The evaluator shall confirm that the procedures documented or referenced in the AM Plan are being followed. AMA_EVD.1.2E

The evaluator shall confirm that the security impact analysis for the current version of the TOE is consistent with the configuration list. AMA_EVD.1.3E

The evaluator shall confirm that all changes documented in the security impact analysis for the current version of the TOE are within the scope of changes covered by the AM Plan. AMA_EVD.1.4E

The evaluator shall confirm that functional testing has been performed on the current version of the TOE, to a degree commensurate with the level of assurance being maintained. AMA_EVD.1.5E

Security Impact analysis (AMA_SIA.1)

The developer security analyst shall, for the current version of the TOE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version. AMA_SIA.1.1D

The security impact analysis shall identify the certified TOE from which the current version of the TOE was derived. AMA_SIA.1.1C

The security impact analysis shall identify all new and modified TOE components that are categorized as TSP-enforcing. AMA_SIA.1.2C

The security impact analysis shall, for each change affecting the security target or TSF representations, briefly describe the change and any effects it has on lower representation levels. AMA_SIA.1.3C

The security impact analysis shall, for each change affecting the security target or TSF representations, identify all IT security functions and all TOE components categorized as TSP-enforcing that are affected by the change. AMA_SIA.1.4C

The security impact analysis shall, for each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change. AMA_SIA.1.5C

The security impact analysis shall, for each applicable assurance requirement in the configuration management (ACM), life cycle support (ALC), delivery and operation (ADO) and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance. AMA_SIA.1.6C

The security impact analysis shall, for each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable. AMA_SIA.1.7C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AMA_SIA.1.1E

The evaluator shall check, by sampling, that the security impact analysis documents changes to an appropriate level of detail, together with appropriate justifications that assurance has been maintained in the current version of the TOE. AMA_SIA.1.2E

5.3 Security Requirements for the IT Environment

ITR_AUD_REV The Mobile Code Enclave will have a considerable amount of auditing. All TOE authorised users shall periodically check these audit data for any security violations.

5.4 Security Requirements for the Non-IT Environment

NITR_PHYSICAL(EXP) The TOE operates within various secure environments, and the equipment requires a certain degree of physical protection. For those equipments operating within the protected area, a degree of physical protection shall be provided in accordance with rules and procedures. For those equipments operating outside the protected area, the user shall provide physical security protections such that the equipments can be operated securely at the corresponding classification level.

NITR_ADMIN_TRAIN(EXP) All network and system administrators shall be trained on all duties associated with their individual roles, including (but not limited to) installing network security components, configuring I&A services, maintaining and reviewing audit data, and managing user accounts.

6— Rationale

6.1 Introduction and TOE Description Rationale

This section provides a set of rationale arguments for the PP.

- Section 6.1 [Introduction and TOE Description Rationale] addresses Threat and Policy coverage by Objectives and Assumptions.
- Section 6.2 addresses [Security Objective Rationale] coverage by TOE and environmental components.
- Section 6.3 addresses the adequacy of the assurance requirements (EAL 2) chosen for this PP.
- Section 6.4 addresses the minimum strength of function issues for this PP.
- Section 6.5 addresses the Dependency coverage for this PP.
- Section 6.6 addresses the comprehensive argument that the PP's IT requirements "form a mutually supportive and internally consistent whole."

6.2 Security Objectives Rationale

This section contains a mapping table and individual arguments for each policy and threat that is covered. Table 6-1 lists either the Organisational Security Policy or Threat that requires coverage in the first column. Relevant and applicable Assumptions are listed in the second column. Objectives that cover each Policy and Threat, given the applicable Assumptions, are listed in the third column. Following this table are individual arguments for the coverage of each Policy and Threat.

Table 6-1 Tracing of Security Objectives to the TOE Security Environment

Policy/Threat	Assumptions	Objectives
P.ACCOUNTABILITY	A.Train	O.Audit, O.I&A, OE.Auditlog, OE.Train
P.AVAILABILITY		O.Interface, OE.Install, OE.Train
P.CONFIDENTIALITY	A.Design, A.Environment, A.Secure, A.Enclave_Integrity, A.Train	O.Audit, O.I&A, O.Protect, OE.Backup, OE.Install, OE.Physical, OE.Train
P.CONFIGURABILITY	A.Design, A.Secure, A.No_Evil, A.Train	O.Audit, O.Detect, O.Policy, O.Protect, OE.Admin, OE.Install
P.DATA	A.Secure	O.All_Data, O.Audit, O.Interface, OE.Admin
P.INTEGRITY	A.Design, A.Environment,	O.Audit, O.Detect, O,I&A, O.Protect, O.Self_Protect,

Policy/Threat	Assumptions	Objectives
	A.Secure	OE.Admin, OE.Backup,
P.INTERFACE	A.Secure	O.Interface, OE.Install, OE.Physical,
P.MANAGE	A.Environment, A.Train	O.Policy, OE.Admin, OE.Auditlog, OE.Install, OE.Physical, OE.Train
P.PORT	A.No_Evil, A.Train	O.Access_Admin, O.All_Data, O.Audit, O.Policy, OE.Train
P.TRAINED	A.Train	OE.Train
T.ACCESS	A.Environment, A.Enclave_Integrity	O.I&A, O.Audit, O.Policy, OE.AuditLog
T.ALTER	A.Environment, A.Secure	O.I&A, O.Self_Protect, OE.Physical, OE.Train
T.AUDFAIL	A.Design, A.Enclave_Integrity, A.No_Evil, A.Train	O.Protect, OE.AuditLog
T.AUDREV	A.Train	OE.Auditlog, OE.Train
T.BACKUP	A.No_Evil, A.Train	O.Protect, OE.Backup, OE.Train
T.DENIAL	A.Enclave_Integrity, A.Environment	O.I&A, O.Self_Protect, OE.Physical,
T.ERROR	A.Train	O.Audit, O.Protect, O.Self_Protect, OE.Train
T.IMPERSONATE	A.Environment	O.Audit, O.I&A, OE.Physical
T.IMPLEMENT	A.Design, A.Secure	O.Audit, OE.Install, OE.Train
T.IMPORT	A.Design, A.Environment,	O.Audit, O.Detect, O.I&A, O.Self_Protect OE.Auditlog, OE.Install
T.INTRUDE	A.Environment, A.Enclave_Integrity	O.Audit, O.I&A, O.Protect, OE.Auditlog
T.MEDIA	A.Environment, A.Secure	O.Protect, O.Self_Protect, OE.Backup, OE.Physical
T.PHYSICAL	A.Environment	OE.Physical
T.REPEAT		O.Audit, O.I&A, OE.Auditlog
T.TRAFFIC	A.Secure	O.Audit, OE.Auditlog, OE.Install, OE.Train
T.TRAIN	A.Train	OE.Train
T.VIRUS	A.No_Evil	O.Audit, O.Detect, O.Self_Protect, OE.Train

6.2.1 Policies

P.ACCOUNTABILITY **User activity will be monitored to the extent that auditing and system controls are applied properly to users, administrators, and system processes.**

Coverage Rationale O.AUDIT will provide an audit trail containing a history of all user activities relevant to TSF and holds administrators responsible for their actions. Components of the system are ensured of their security by using identification and authentication of administrators (O.I&A) in the support system. Through OE.AUDITLOG, the administrator must provide proper management and review of the TOE to maintain system security. OE.TRAIN requires that the individual be properly trained on the operations of the TOE and its associated security functions. A.TRAIN assumes that all authorized personnel are properly trained on operational procedures of the TOE.

P.AVAILABILITY **The TOE will provide timely, reliable access to information and system resources to meet mission planning requirements.**

Coverage Rationale O.INTERFACE will ensure information access security by providing a connection between external and internal networks. A properly set up and managed TOE (OE.INSTALL) will allow the proper information be provided to enhance mission capability. OE.TRAIN ensures secure information by providing training for authorised personnel.

P.CONFIDENTIALITY **The TOE will provide security features assuring that information is not disclosed to unauthorised persons, processes, or devices.**

Coverage Rationale O.AUDIT assures recording of relevant security events to prevent unauthorised access of secure information. All individuals using the system are uniquely identified and authenticated (O.I&A) to prevent unauthorised access. O.PROTECT will secure data from unauthorized persons in the event of system failure. OE.BACKUP provides frequent system checks to be performed to ensure information confidentiality. OE.INSTALL provides a secure system during installation in order to prevent information access into the system. The TOE is expected to be physically protected (OE.PHYSICAL) from any unauthorised persons. OE.TRAIN provides effective training of security policies and procedures to enhance confidentiality of information. A.DESIGN assumes the system is void of any malfunctions during manufacturing and delivery of the system to avoid unauthorised system access. A.ENVIRONMENT also assumes that the system remains in a secure location to protect against tampering. A.SECURE assumes the system is configured correctly and will operate in that configuration to prevent unauthorised access. The

assumption that the communication between the TOE and users operates in a secure environment will maintain information confidentiality (A.ENCLAVE_INTEGRITY). The assumption that authorised persons are properly trained to maintain information confidentiality is covered under A.TRAIN.

P.CONFIGURABILITY **The TOE will provide configurations of allowable policies of the TOE definable at the system, group, or user levels.**

Coverage Rationale O.AUDIT ensures the security of the TOE by detecting and recording any misconfiguration of the TOE, which could lead to network susceptibility. O.DETECT will detect unauthorised changes to the systems configuration. O.POLICY provides security of the TOE through documentation of administrative policies. O.PROTECT protects configuration of the system when the system, component, or power failure occurs. The TOE must be configured by administrators to support the system's security policies at all levels (OE.ADMIN). Proper installation and configuration of the TOE depends on security management and operational techniques (OE.INSTALL). It is assumed that the system is configured correctly and void of malfunctions during manufacturing (A.DESIGN). It is assumed that the system is configured (A.SECURE) properly to ensure a secure TOE. It is also assumed that administrators will not deliberately harm the system (A.NO_EVIL). All administrators are assumed to be properly trained on TOE policies and operational procedures (A.TRAIN).

P.DATA **The network and host on which the TOE is installed will be configured to route all applicable data through the TOE to ensure that the TSP will be met.**

Coverage Rationale O.ALL_DATA ensures that all data received will be scanned to protect target security of the TOE. O.AUDIT will detect any attack or misconfiguration against the TOE enhancing security of TSP. The interaction between external and internal networks will remain secure to ensure the TSP is achieved (O.INTERFACE). Administrators will configure and manage policies concerning TOE data to protect the TSP (OE.ADMIN). It is assumed that the TOE and all system resources will operate in the correct configuration (established by an accredited source) to enable the TSP to be met (A.SECURE).

P.INTEGRITY **The TOE will provide controls to protect the integrity of information and system resources, including maintaining the integrity of the TSF in the event of a system failure (e.g. fail-safe).**

Coverage Rationale The integrity of the system will be enhanced by ensuring that audit trails (O.AUDIT) are kept for tracking and detecting any breach in security. If the system fails, the TOE will detect any modifications done to the protected data (O.DETECT). All administrators will also be identified and authenticated (O.I&A) to ensure the TOE is operated by authorised personnel. (O.PROTECT) ensures the security of the TSF and it's information in the event of system or component failure and will protect TOE information by preventing automated malicious codes into the system (O.SELF_PROTECT). Administrators will manage security policies in accordance with the TOE (OE.ADMIN) to ensure information remains secure. The TOE will automatically execute periodic check-ups (OE.BACKUP) to enhance the security of classified resources. It is assumed that the manufacturing of the TOE (A.DESIGN) will maintain secure information and comply with security specifications of the TOE. It is assumed that the TOE will be located in a secure environment to minimise the risk of an unauthorised user (A.ENVIRONMENT). It is also assumed that the TOE is functioning properly and TSF are configured correctly (A.SECURE).

P.INTERFACE **All incoming interfaces to the TOE are subject to the TSP defined for the TOE.**

Coverage Rational: The TOE must interface with other entities (O.INTERFACE) located inside the enclave and possibly outside. Proper installation and management (OE.INSTALL) of the system will ensure the TOE will comply with the communication and security of other systems. All interfaces will also be physically protected (OE.PHYSICAL) to ensure that security is not compromised. When an interface with another system occurs, all systems linked to the TOE system are assumed to be configured correctly (A.SECURE).

P.MANAGE **The TOE will be managed such that the TSFs are properly activated, implemented and preserved throughout its operational lifetime.**

Coverage Rationale O.POLICY provides documentation for administrators to access the TOE for secure implementation of the TSF. Security functions that implement protection on the system must be managed and configured by administrators to TOE security policies (OE.ADMIN). Adequate management of the TOE depends on proper installation of security enforcement and security management functions (OE.INSTALL) and the management of audit facilities to safeguard data (OE.AUDITLOG). Adequate management of the TOE requires physical protection (OE.PHYSICAL) to protect the TSF from unauthorised access. OE.TRAIN provides appropriate training to authorised personnel to manage the security of the TSF. It is assumed that the TOE is located in a secure environment to enhance TSF security management

(A.ENVIRONMENT). It is also assumed that authorised personnel are properly trained (A.TRAIN) to manage the TSF.

P.PORT **Administrators of the TOE will not import or export TSF data without proper and explicit authorisation.**

Coverage Rationale O.ACCESS_ADMIN provides access to administrators from within the TOE authorising them to proceed with any transactions. O.ALL_DATA shall verify all data incoming to enhance TOE security of TSF data. O.AUDIT will keep track of tasks done by the administrators that can be verified if improper security procedures occur and hold administrators accountable for their actions. O.POLICY provides access policies to administrators prior to any import or export of data. An objective of a training environment will ensure that continued training for its administrators will minimise improper operation of the TSF (OE.TRAIN). (A.NO_EVIL) assumes that administrators will not intentionally compromise the TOE with improper data transactions. It is also assumed that administrators are trained and competent to protect all data within security policies of the TOE (A.TRAIN).

P.TRAINED **All TOE administrators will be properly trained on the TSF prior to accessing an operational TOE.**

Coverage Rationale All administrators must be adequately trained and cleared before operation and management of a TOE will be accessible (OE.TRAIN). It is assumed that system administrators are properly trained before their access to an operational TOE (A.TRAIN).

6.2.2 Threats

T.ACCESS **An unauthorised individual may surreptitiously gain access to the TOE administrative functions by utilising vendor proprietary maintenance mechanisms and/or pre-established user accounts.**

Coverage Rationale: (O.I&A) protects the TOE from illegal access with strict identification and authentication mechanisms to prevent altering or compromise to the system. The TOE provides mechanisms for setting adminstor access policy (O.POLICY). Administrator actions are audited (O.AUDIT) and the audit logs are reviewed regularly (OE.AUDITLOG). The TOE runs in an enclave that assures integrity of intra-enclave communication (A.ENCLAVE_INTEGRITY). The assumption (A.ENVIRONMENT) further counters this threat by assuming a controlled access environment, which provides additional physical protection for the TOE.

T.ALTER	**An unauthorised individual may surreptitiously gain access to the TOE and attempt to alter and/or replace system elements (e.g. hardware, firmware, or software and data) and thereby compromise the TOE.**
Coverage Rationale:	(O.I&A) protects the TOE from illegal access with strict identification and authentication mechanisms to prevent altering or compromise to the system. The TOE will protect the TSF against unauthorised modifications (O.SELF_PROTECT). There will be environmental support for the TOE (OE.PHYSICAL) to provide protection from physical attack for security critical parts of the TOE. The assumption (A.ENVIRONMENT) further counters this threat by assuming a controlled access environment, which provides additional physical protection for the TOE. All administrators must be properly trained in operation and policies of the TOE (OE.TRAIN). It is assumed that the TOE will operate in a secure manner and configuration to prevent unauthorised access and potential threat to the system (A.SECURE).
T.AUDFAIL	**System modification, compromise, or audit file "full" may result in failure to collect audit data.**
Coverage Rationale	O.PROTECT ensures that the documented audit data is properly protected. OE.AUDITLOG places the responsibility on security administrators to document audit data on a regular basis to prevent audit trail exhaustion. It is assumed that the TOE will have sufficient audit logging capability to meet the TSF (A.DESIGN). It is assumed that the communication process between administrator and system provides protection from modification to inhibit data collection (A.ENCLAVE_INTEGRITY). It is also assumed that administrators will not intentionally degrade the system to prevent collection of data (A.NO_EVIL). A.TRAIN assumes that system administrators are well trained and aware of audit data policies governed by the TOE.
T.AUDREV	**Appropriate individuals may fail to adequately review and interpret audit data or take appropriate action.**
Coverage Rationale	OE.AUDITLOG places the responsibility on security administrators to inspect audit data on a regular basis, and to take appropriate action on the detection of a breach in security, or events that can lead to a breach in security. OE.TRAIN ensures administrators are trained on TOE security functions, and procedures requiring review audit data. It is assumed that the authorised personnel are adequately trained to review audit data (A.TRAIN).

T.BACKUP	**Failure to adequately perform system backup of TOE Security Function (TSF) data may result in compromise or non-availability of the TOE.**
Coverage Rationale	O.PROTECT ensures that the archived data is properly protected. OE.BACKUP provides environmental support to mitigate this threat by requiring periodic backups of security-critical TOE resources, including TSF data. OE.TRAIN ensures administrators are trained on the proper operation of TOE security functions. It is assumed that system administrators will not plan to corrupt the TOE or TSF data (A.NO_EVIL). It is also assumed that trained personnel are competent with the operation of TOE security functions (A.TRAIN).
T.DENIAL	**An unauthorised user may render the TOE systems unavailable for use.**
Coverage Rationale:	O.I&A can mitigate this threat by limiting unauthorised access to the system through stringent identification and authentication methods. Administrators must be able to physically protect network resources, so as to prevent intentional or unintentional denial of service (OE.PHYSICAL). A.ENVIRONMENT provides a controlled access environment to protect against unauthorised physical access by attackers attempting system attacks. Communication of TOE systems with administrators operates in a controlled environment (A.ENCLAVE_INTEGRITY) to prevent unauthorised access to the system. Lastly, the TOE protects itself from malicious mobile code (O.SELF_PROTECT).
T.ERROR	**An authorised administrator performs erroneous actions that will compromise administrator and/or system resources.**
Coverage Rationale:	The audit data requirements on the individual IT systems within the TOE will ensure that errors will be recorded (O.AUDIT). The system will prevent further security violations by limiting its error to the operations of that particular IT system within the TOE and protecting the rest of the system (O.PROTECT and O.SELF_PROTECT). Administrators must undergo training on the system and on the operation of the TSF (OE.TRAIN). It is assumed that authorised personnel are suitably trained to minimise erroneous actions (A.TRAIN).
T.IMPERSONATE	**An unauthorised user may attempt to gain access to the TOE by pretending to be an authorised user.**
Coverage Rationale	O.AUDIT will provide the administrators the capability to trace and record user activities on the TOE. The TOE will employ strong identification and authentication mechanisms to reduce security breach of the TOE (O.I&A). The TOE is expected to be physically protected from

unauthorised users (OE.PHYSICAL). A.ENVIRONMENT states that the TOE will be in a secure environment limiting physical access to the TOE.

T.IMPLEMENT **Due to the implementation process, the TOE may have intentional or unintentional errors that may allow unauthorised access.**

Coverage Rationale: O.AUDIT requires all information be recorded and secure from unauthorised access and renders responsibility to administrators for erroneous actions. During installation of the TOE components, authorised administrators will configure the TSF in accordance with vendor provided guidance (OE.INSTALL). During the implementation and configuration process, administrators must be trained (OE.TRAIN) on TSF and proper procedures. A.DESIGN assumes that the system will comply with all security requirements preventing unauthorised accessibility to the system. It's assumed that the TOE will operate in a secure manner to prevent unauthorised actions (A.SECURE).

T.IMPORT **Malicious code may be introduced into the system, resulting in a compromise of the integrity and/or availability of the TOE.**

Coverage Rationale Administrators and managers will use audit logs to trace and hold accountable any unauthorised user who introduces malicious code into the TOE (O.AUDIT, OE.AUDITLOG). O.DETECT will detect any malicious code activity and send a warning to the administrator. The TOE will protect its TSF data (O.SELF_PROTECT) in the event that malicious code is detected. The TOE will be delivered for installation without embedded malicious code (A.DESIGN), to include all system updates during the operational lifetime of the TOE (OE.INSTALL). To protect the TOE from malicious code, access to the TOE is limited by the controlled access environment (A.ENVIRONMENT) and by strong identification and authentication mechanisms (O.I&A). These safeguards ensure that malicious codes are minimised in the TOE network.

T.INTRUDE **An unauthorised user may gain access to one or more components of the TOE or the TOE network from an outside network.**

Coverage Rationale The TOE will employ strong identification and authentication mechanisms to ensure that only authorised users gain access to the TOE network (O.I&A). The system administrators and managers will utilize the system auditlogs to trace unauthorized activities and reconfigure the system as necessary to prevent similar compromises in the future (O.AUDIT, OE.AUDITLOG). The TOE will protect local and remote data storage areas against intrusion (O.PROTECT). The environment of the TOE must be in a physically secure location (A.ENVIRONMENT) to prevent unauthorised access to the hardware. A.ENCLAVE_INTEGRITY enables

	the system to maintain a high level of security for communications between the TOE and administrator to limit unauthorised access.
T.MEDIA	**Failure to adequately protect storage media may result in compromise or non-availability of the TOE.**
Coverage Rationale	TOE media will be handled at the appropriate levels of sensitivity (O.PROTECT, A.SECURE) All data will be reviewed on a periodic basis (OE.BACKUP). O.SELF_PROTECT gives the TOE the ability to protect itself from malicious codes that may disrupt storage protection. The TOE is located in a secure facility (A.ENVIRONMENT) and its critical components are protected from physical attack (OE.PHYSICAL); these safeguards mitigate the threat to the TOE's media.
T.PHYSICAL	**Security-critical parts of the TOE may be subject to physical attack or enemy capture that may compromise security.**
Coverage Rationale	The TOE is located in a secure facility (A.ENVIRONMENT) and its critical components are protected from physical attack (OE.PHYSICAL).
T.REPEAT	**An unauthorised user may repeatedly attempt to guess authentication information.**
Coverage Rationale	The system administrators and managers will utilize the system audit logs to trace repeated unsuccessful access attempts and reconfigure the system as necessary to prevent compromises of the TOE (O.AUDIT and OE.AUDITLOG). In order to protect the TOE from repeated attempts to guess authentication information, each administrator will be uniquely identified and authenticated prior to use (O.I&A).
T.TRAFFIC	**Use of the TOE may unintentionally transmit sensitive information to unauthorised users.**
Coverage Rationale	Adequate audit capabilities within the TOE should reveal indications of unauthorized search activities (O.AUDIT). The TOE will also have the ability to audit and manage its extent of remote management services (OE.AUDITLOG). Before the TOE is accredited, it must be installed and operated in a manner that maintains the system security (OE.INSTALL). A.SECURE assumes that the accredited system configuration will mitigate the ability for someone to launch an unsophisticated sweep of a network. OE.TRAIN provides sufficient training on TOE security functions and policies.
T.TRAIN	**Insufficient user training on TOE security features may result in system vulnerabilities.**

Coverage Rationale — Administrators are trained on the proper operation of all TOE security functions to ensure system protection (OE.TRAIN). A.TRAIN assumes that all authorised personnel are sufficiently trained to perform on the operational TOE system.

T.VIRUS — **An authorised user may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of the TOE.**

Coverage Rationale — The TOE and administrators will use audit logs to trace and hold accountable any authorised administrator who introduces malicious code into the TOE (O.AUDIT). O.DETECT will identify and mitigate any malicious codes in the system and alert administrators immediately. The TOE will protect itself in the event of malicious codes involving the security of the system and warn the administrator to take action (O.SELF_PROTECT). Administrators will be trained on methods and procedures in order to prevent introduction of malicious code into the system (OE.TRAIN). It is assumed that administrators will not willingly attempt to compromise the TOE or TSP with viruses or other malicious codes (A.NO_EVIL).

6.3 Security Requirements Rationale

6.3.1 Functional Security Requirements Rationale

This section contains a mapping table and individual arguments for each Objective covered. Table 6-2 lists either the TOE or Environmental Objective that requires coverage in the first column. TOE components and/or environmental requirements that cover each Objective are listed in the second column. Following this table are individual arguments for the coverage of each Objective.

Table 6-2 Functional Component to Security Objective Mapping

Objectives	Requirements
O.ACCESS_ADMIN	FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMR.1, FTA_TSE.1
O.ACCESS_USER	FDP_ACC.2, FDP_ACF.1, FDP_ITC.2, FIA_UAU.1, FIA_UID.1
O.ALL_DATA	FAU_GEN.1, FAU_GEN.2, FCS_CKM.3, FDP_ITC.1, FDP_ITC.2, FDP_RIP.2
O.AUDIT	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SEL.1, FIA_AFL.1, FIA_USB.1, FPT_AMT.1, FPT_STM.1
O.DETECT	FAU_ARP.1, FAU_SAA.1, FDP_ACC.2, FDP_AFC.1, FIA_AFL.1, FPT_TST.1,
O.I&A	FIA_AFL.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FMT_MSA.2, FMT_MSA.3, FTA_SSL.3

Objectives	Requirements
O.INTERFACE	FDP_ITC.2, FPT_ITA.1, FPT_TDC.1, FTP_TRP.1
O.POLICY	FCS_COP.1, FDP_ACC.2, FDP_ACF.1, FDP_IFC.2, FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FTA_LSA.1, FTA_MCS.1, FTA_SSL.3, FTA_TSE.1
O.PROTECT	FAU_STG.1, FAU_STG.3, FDP_IFF.1, FDP_RIP.2, FPT_FLS.1,
O.SELF_PROTECT	FAU_ARP.1, FAU_SAA.1, FDP_RIP.2, FIA_AFL.1, FIA_SOS.1, FIA_UAU.7, FPT_FLS.1, FPT_RCV.2, FPT_RVM.1, FPT_SEP.1, FPT_TST.1
OE.ADMIN	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SEL.1, FAU_STG.3, FDP_ACC.2, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1, FIA_USB.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMR.1, FPT_AMT.1, FTA_LSA.1, FTA_MCS.1
OE.AUDITLOG	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SEL.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FPT_AMT.1, ITR_AUD_REV
OE.BACKUP	FPT_RCV.2, FPT_RVM.1, FPT_TST.1
OE.INSTALL	FPT_STM.1, NITR_ADMIN_TRAIN
OE.PHYSICAL	NITR_PHYSICAL
OE.TRAIN	ITR_AUD_REV, NITR_ADMIN_TRAIN

O.ACCESS_ADMIN **Administrators access can be either from within the TOE or within enclave.**

Coverage Rationale The TSF will enforce access based on security attributes that will allow administrators to access the system (FDP_ACF.1) in a secure manner. FMT_MOF.1 allows authorised personnel to access the TOE, take on an administrator role and manage necessary functions for proper operation. FMT_MSA.1 enables TOE system access by administrators for capability to manage security attributes. Managers must have access to the system in order to properly manage TSF data (FMT_MTD.1). There are specific TSF security guidelines that administrators must follow for proper management (FMT_SMR.1) and access to the system. FTA_TSE.1 requires management of administrator system establishment, including setting addresses from which remote administration is permitted.

O.ACCESS_USER **The TOE will be configured such that all users within the enclave will be subject to the policy of the TSP.**

Coverage Rationale System personnel must follow strict guidelines (FDP_ACC.2) in the access control policy regarding SFP access. FDP_ACF.1 provides

functions that are implemented along with the FDP_ACC.2 policy to enforce access based upon security attributes. The FDP_ITC.2 function requires administrators to abide by TSP policies and protect user data within the TOE. All TOE users must perform certain actions (FIA_UAU.1) prior to taking advantage of the TSF. FIA_UID.1 requires all administrators to perform actions according to policies by the TSF before access is granted.

O.ALL_DATA **The TOE will scan all data received. (See Section 2 "TOE Description")**

Coverage Rationale The TOE will inspect all data and apply the rules in the TSP in deciding how to process it (FDP_IFC.2, FDP_ITC.2) The TOE will record all auditable information about the data items it processes (FAU_GEN.2). The TOE will authenticate any incoming information that possesses a cryptographic signature (i.e. signed mobile code), identifying and validating the identity of the source (FDP_DAU.2); the TOE will employ public-key cryptography for this, managing the public key certificates in a manner consistent with the X.509 and other relevant standards (FCS_CKM.3). The TOE will ensure that all local data storage resources, including cache, utilized by data items are completely cleared of previous contents before re-use (FDP_RIP.2). FCS_CKM.3 provides for secure and proper handling of public keys used for signature verification of signed mobile code.

O.AUDIT **TOE will provide means of recording any security relevant events, so as to assist an administrator in detection of potential attacks or misconfiguration of the TOE security features that would leave the network susceptible to attack, and also hold administrators accountable for any actions they perform that are relevant to security.**

Coverage Rationale Mechanisms are devised to provide alarms (FAU_SAA.1), so administrators can react to identified attacks covered by (FAU_ARP.1). This mechanism will enhance the reaction time of security relevant events. FAU_GEN.1 is the primary requirement that specifies details in auditable events. Administrator actions are associated with system processes through the inclusion of FAU_GEN.2. The TSF provides administrators the capability to interpret audit records generated by the TOE (FAU_SAR.1). Accessing auditable data must be restricted from other personnel in the enclave, who may not be authorized for such data (FAU_SAR.2). The TOE supports audit review by allowing an administrator to include or exclude particular events, thus enhancing the ability of the administrator to detect security anomalies. FIA_AFL.1 provides security through auditable events such as failed login attempts.

	Any subjects acting on an administrator's behalf may be audited (FIA_USB.1) and held responsible for their actions. FPT_AMT.1 managed by administrators will provide initial system testing for security violations to the TOE. FPT_STM.1 provides reliable time stamps for the TSF audit functions.
O.DETECT	**The TOE will detect and mitigate malicious mobile code.**
Coverage Rationale	FAU_SAA.1 will assist in detecting security violations and FAU_ARP.1 mechanisms will alert the administrator that the configuration of the system has been compromised. FIA_AFL.1 will also provide indications of unauthorised access attempts to the TOE. FPT_TST.1 through self-tests will detect any malicious attack to data in the TOE. The TOE will scan all incoming data for mobile so that it can apply the relevant TSP rules (FDP_ACC.2 and FDP_AFC.1).
O.I&A	**Security components and critical network components will be protected by strong identification and authentication mechanisms. These mechanisms will identify all administrators and will authenticate the claimed identity before granting an administrator access to the TOE network.**
Coverage Rationale	FIA_AFL.1 enables the system to terminate after a specified number of unsuccessful attempts to enter the TOE, and will disable the individuals account from the system of entry. The TSF provides a mechanism (FIA_SOS.1) for I&A through verification of secrets. Specific actions must be performed for authentication before access to the TOE is accepted (FIA_UAU.1). Authenticated administrators will receive minimal feedback information to further protect the limited feedback security feature (FIA_UAU.7). Proper identification requires certain actions be performed before access to the system is granted (FIA_UID.1). FMT_MSA.2 requires the system to maintain and secure validated data of its security attributes. FMT_MSA.3 ensures that the system remains secure during initialisation to mitigate the threat of unauthorised access. FTA_SSL.3 shortens the time window for compromises by terminating a session after a period of non-use.
O.INTERFACE	**The TOE must support the capability to interface with gateways connected to external networks and internal enclave networks. (REMOTE USERS)**

Coverage Rationale The TOE provides a link between internal enclave clients, users, and external information sources. To perform this job securely, it must be able to interface with external gateways and accept data items from them for scanning (FDP_ITC.2). The TOE must be able to accept data items from these external gateways whenever the necessary network connectivity exists (FPT_ITA.1). The TOE may not transfer data without imposing the relevant TSP rules, not even at the direction of external gateways (FPT_RVM.1). The TOE must remain in a secure state during interaction with external gateways, including trusted ones (FPT_TDC.1). FTP_TRP.1 will support a trusted path between administrators and the TSF to increase protection of TOE information.

O.POLICY **The TOE will support both the administrative access policies and malicious mobile code policies.**

Coverage Rationale FDP_ACC.2 will ensure the security of the TOE through correct policies and regulations. The TSF shall be able to accept and enforce rules about mobile code formats to detect and what actions to take upon detection of them (FDP_ACF.1). To prevent malicious mobile coding, FDP_IFC.2 require that all information flows and operations within the TSC be in place for a subset of operations and be covered by one SFP. FIA_ATD.1 provides a policy that defines requirements associated with attributes needed to enforce the TSP. FIA_UAU.1 and FIA_UAU.7 maintain policies regarding authentication procedures supported by the TSF. Action performing identification procedures are defined in the policy covered by FIA_UID.1. TOE governed policies contain requirements limiting the scope of session secure attributes (FTA_LSA.1). The FTA_MCS.1 requirement will limit the number of concurrent sessions an individual can maintain at one time to prevent unauthorised use. TSF policies can prevent unauthorised access and malicious code by terminating a session after a period of inactivity (FTA_SSL.3). FTA_TSE.1 governs a policy that denies administrator access to the TOE based on attributes that limit unauthorised access. FCS_COP.1 supports access policies to configure cryptographic operations according to assigned standards for protection of digital signatures.

O.PROTECT **The TOE will ensure the protection of its TSF and storage. This protection will include the following:**

1) **Fail Safe capability**
2) **Secure initialisation with the event unplanned power outage**

Coverage Rationale Audit data storage will be protected against unauthorised modification or misuse (FAU_STG.1). FAU_STG.3 specifies action to be taken in the event that an audit trail is exceeded to prevent audit data loss. All residual information in the TSF will remain secure and unavailable when reallocating a system resource (FDP_RIP.2). The TSF will remain in a secure state in the event of any identifiable system failure (FPT_FLS.1) to eliminate a breach of security.

O.SELF_PROTECT The TOE will provide a means to protect itself from automated malicious mobile code by blocking the code and display a warning to the administrator for immediate action. The TOE will also have a capability to update itself against new malicious mobile code threats.

Coverage Rationale The TSF shall activate an alarm (FAU_SAA.1) in the event there is a potential security violation and notify TOE authorities for necessary action (FAU_ARP.1). The TSF shall maintain itself in a secure format for residual information when it is being reallocated (FDP_RIP.2). FIA_AFL.1 protects the TSF by terminating usage after a certain number of unsuccessful authentication attempts. The TSF shall verify secrets that meet requirements for system protection (FIA_SOS.1). The TSF shall minimise authentication feedback for personnel to prevent any malicious coding techniques (FIA_UAU.7). In the event that the system fails or shuts down, the TOE will maintain security of its data and functions (FPT_FLS.1). The automatic recovery mechanism enables the TOE to return to a secure state when the system discontinues operation for a period of time (FPT_RCV.2). The TSF shall ensure the rules in the TSP are properly applied to each data item before that item is transferred out of the TOE; if some portion of the TSP cannot be applied due to compromise of that part of the TSF, then the data item shall not be stored in the TOE not forwarded to the user (FPT_RVM.1). The TOE shall maintain a secure domain for its own execution, protecting itself from unauthorized modification or tampering by other users and processes on its host system (FPT_SEP.1). FPT_TST.1 provides random self-testing of the system to verify data integrity and proper TSF operation.

OE.ADMIN The administrator will plan, configure, audit, and manage policies at both system and user levels.

Coverage Rationale FAU_GEN.1 authorises administrators to manage auditable data according to policies at any level and identify the subject associated with those events (FAU_GEN.2). The capability for administrators to review audit

records is covered by FAU_SAR.1, and FAU_SAR.2 limits the number of authorised individuals who can read this information. TOE administrators shall manage auditable events (FAU_SEL.1) as to include or exclude certain information appropriate for security of the TOE. TOE administrators will take appropriate actions necessary (FAU_STG.3) in the event data is lost or audit trails are exceeded to ensure system security. TOE administrators will manage access control policies at system levels to enhance TOE security (FDP_ACC.2). All access control functions will be managed in a way that will prevent unauthorised access into the system (FDP_ACF.1). The TOE must provide an administrative interface that ensures that all information flows handled by the TSF are configured with rules in the TSP (FDP_IFC.2). FDP_IFF.1 allows administrators to set rules to manage the information flow function in order to prevent any policy violations. Authorised administrators shall manage and maintain an association between administrators and subjects acting on their behalf (FIA_USB.1). FMT_MOF.1 allows management of functional behaviour under specified conditions and regulations. Administrators shall accept only valid security attributes, manage those attributes (FMT_MSA.1, FMT_MSA.2) and review or modify them if necessary to enhance the security of the TOE. They must also ensure that these attributes are kept either permissive or restrictive in nature (FMT_MSA.3). FMT_MTD.1 requires administrators to manage TSF data and take appropriate action if limits on TSF data are exceeded. TOE administrators shall revoke security attributes (FMT_REV.1) when necessary to further provide a secure system. Security management guidelines are specified (FMT_SMR.1) for administrators with respect to their roles of responsibility within the TSF. Administrators are responsible testing the system at initial start up for security infractions at system level (FPT_AMT.1). Limiting the scope of session security attributes that one may select will be controlled by system administrators (FTA_LSA.1). Administrators shall manage the TSF in a way that limits concurrent sessions by the same user (FTA_MCS.1).

OE.AUDITLOG **Administrators of the TOE must ensure audit facilities are used and managed effectively.**

Coverage Rationale Authorised personnel will ensure proper actions to be taken (FAU_ARP.1) in the event a security violation is detected (FAU_SAA.1). TOE administrators will ensure that auditable events are properly recorded (FAU_GEN.1), and identify users and their audited events to provide accountability (FAU_GEN.2). A limited number of TOE administrators that review auditlogs and its contents to enhance information security is covered by FAU_SAR.1 and FAU_SAR.2. System administrators will manage audit data to include or exclude events (FAU_SEL.1) within TOE guidelines to ensure proper TOE operation. Functional management is

required by administrators to securely authenticate audit functions in the TSF (FMT_MOF.1). FMT_MSA.1 and FMT_MSA.3 cover administrative management for security attributes and ensure that they remain either permissive or restrictive in nature. FPT_AMT.1 ensures that administrators will properly manage the testing of security measures within the TSF. ITR_AUD_REV requires administrators to regularly review the audit logs and revise the TSP accordingly to maintain the security of the TOE.

OE.BACKUP **Periodic backups will be performed to protect security-critical TOE resources.**

Coverage Rationale During backup procedures, the TOE shall not enter an insecure operational state – it may suspend operations or it may continue operating in a secure state (FPT_RCV.2). A backup system check may be performed as a part of initialization, to prevent operation of the TOE when backup facilities are unavailable (FPT_RVM.1). FPT_TST.1 enables the system to perform self-tests to ensure proper operation of the TOE as well as verifying data integrity of the TSF.

OE.INSTALL **Those responsible for the TOE must ensure the TOE is delivered, installed, managed and operated in a manner which maintains the system security.**

Coverage Rationale The FPT_STM.1 function will ensure that a reliable time source is referenced by the TOE during installation and operation of the system. Proper training in TOE initial configuration and maintenance, including audit review procedures, will ensure security of the TOE during installation and operation (NITR.ADMIN_TRAIN).

OE.PHYSICAL **Those responsible for the TOE must ensure that parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.**

Coverage Rationale The functional requirement NITR_PHYSICAL ensures that all personnel associated within the TOE environment follow security guidelines and protect the system from any physical attack.

OE.TRAIN **Authorised administrators are trained on the proper operation of TOE security functions. Additionally, TOE security parameters are**

	established by administrators according to security policies and parameters.
Coverage Rationale	Authorised administrators of the TOE must be properly trained for reviewing audit procedures according to ITR_AUD_REV policy. NITR_ADMIN_TRAIN function requires authorised administrators to be properly trained for correct installation and operational procedures on the TOE.

6.3.2 Assurance Security Requirements Rationale

Based on the threats and required Strength of Function (SOF) discussed in Section 3.2 Threats to Security, the security critical components of the Mobile Code Enclave shall meet a minimum NIAP evaluated assurance level (EAL) of 2. Certain components, as determined by the Mobile Code Enclave team and Program Office, may require a higher EAL. Those components requiring a High SOF as described in ALC_FLR and AVA_CCA, and require an EAL greater than 2.

In order to provide the necessary support to the Mobile Code Enclave, Flaw Remediation and Maintenance of Assurance requirements augment the assurance requirements for EAL 2. The integrator shall provide a mechanism to correct flaws in the TOE that are discovered after initial delivery and installation. As a result of modifications, fixes, or other changes to the accredited TOE configuration, the TOE may require additional processes/evaluations to maintain DAA and/or NIAP accreditation. Thus, the Maintenance of Assurance class of requirements are required.

Mobile Code Enclave Security Products may be considered for use in high assurance systems. The following guidance was used to determine the EAL for Mobile Code Enclave Security Products.

- Global Information Grid (GIG) Policy
- DOD/CIO Guidance 6-8510 dtd January 5, 2000

Although, the GIG policy states that an EAL 2 is required for a high assurance system, the Mobile Code Enclave as a whole has an EAL 2. Certain subsystems making the Support System may require an EAL 2 or higher. Augmented assurance requirements mentioned above gives guidelines to specific areas that need an EAL 2 or higher.

6.4 Dependency Rationale

Table 6-3 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_ARP.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAA.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1
FCS_CKM.3	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2
FDP_ACC.2	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_IFC.2	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1_FTP_TRP.1], FPT_TDC.1
FDP.RIP.2	NONE
FIA_AFL.1	FIA_UAU.1
FIA_ATD.1	NONE
FIA_SOS.1	NONE
FIA_UAU.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1
FIA_UID.1	NONE
FIA_USB.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1

Requirement	Dependencies
FMT_MTD.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1
FMT_REV.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1
FPT_AMT.1	NONE
FPT_FLS.1	ADV_SPM.1
FPT_ITA.1	NONE
FPT_RCV.2	ADV_SPM.1, AGD_ADM.1, FPT_TST.1
FPT_RVM.1	NONE
FPT_SEP.1	NONE
FPT_STM.1	NONE
FPT_TDC.1	NONE
FPT_TST.1	FPT_AMT.1
FTA_LSA.1	NONE
FTA_MCS.1	FIA_UID.1
FTA_SSL.3	NONE
FTA_TSE.1	NONE
FTP_TRP.1	NONE
ITR_AUD_REV	NONE
NITR_ADMIN_TRAIN	NONE
NITR_PHYSICAL	NONE

6.5 Security Functional Requirements Grounding in Objectives

All the security functional requirements in the protection profile have a basis in the security objectives of the TOE, as indicated in the following table.

Table 6-4 Requirements to Objectives Mapping

Requirements	Objectives
FAU_ARP.1	O.AUDIT, O.DETECT, O.SELF_PROTECT, OE.AUDITLOG
FAU_GEN.1	O.ALL_DATA, O.AUDIT, OE.ADMIN, OE.AUDITLOG
FAU_GEN.2	O.ALL_DATA, O.AUDIT, OE.ADMIN, OE.AUDITLOG
FAU_SAA.1	O.AUDIT, O.DETECT, O.SELF_PROTECT, OE.AUDITLOG

Requirements	Objectives
FAU_SAR.1	O.AUDIT, OE.ADMIN, OE.AUDITLOG
FAU_SAR.2	O.AUDIT, OE.ADMIN, OE.AUDITLOG
FAU_SEL.1	O.AUDIT, OE.ADMIN, OE.AUDITLOG
FAU_STG.1	O.PROTECT
FAU_STG.3	O.PROTECT, OE.ADMIN
FCS_CKM.1	O.ALL_DATA
FCS_CKM.3	O.ALL_DATA
FCS_CKM.4	O.ALL_DATA
FCS_COP.1	OE.ADMIN
FDP_ACC.1	O.ACCESS_USER, O.POLICY, OE.ADMIN
FDP_ACC.2	O.ACCESS_USER, O.POLICY, OE.ADMIN
FDP_ACF.1	O.ACCESS_ADMIN, O.ACCESS_USER, O.POLICY, OE.ADMIN
FDP_IFC.2	O.POLICY, OE.ADMIN
FDP_IFF.1	O.PROTECT, OE.ADMIN
FDP_ITC.1	O.ALL_DATA
FDP_ITC.2	O.ACCESS_USER, O.ALL_DATA, O.INTERFACE
FDP.RIP.2	O.ALL_DATA, O.PROTECT, O.SELF_PROTECT
FIA_AFL.1	O.AUDIT, O.DETECT, O. I&A, O.SELF_PROTECT
FIA_ATD.1	O.POLICY
FIA_SOS.1	O.I&A, O.SELF_PROTECT
FIA_UAU.1	O.ACCESS_USER, O.I&A, O.POLICY
FIA_UAU.7	O.I&A, O.POLICY, O.SELF_PROTECT
FIA_UID.1	O.ACCESS_USER, O.I&A,, O.POLICY
FIA_USB.1	O.AUDIT, OE.ADMIN
FMT_MOF.1	O.ACCESS_ADMIN, OE.ADMIN, OE.AUDITLOG
FMT_MSA.1	O.ACCESS_ADMIN, OE.ADMIN, OE.AUDITLOG
FMT_MSA.2	O.I&A, OE.ADMIN
FMT_MSA.3	O.I&A, OE.ADMIN, OE.AUDITLOG
FMT_MTD.1	O.ACCESS_ADMIN, OE.ADMIN
FMT_REV.1	OE.ADMIN
FMT_SMR.1	O.ACCESS_ADMIN, OE.ADMIN
FPT_AMT.1	O.AUDIT, OE.ADMIN, OE.AUDITLOG
FPT_FLS.1	O.PROTECT, O.SELF_PROTECT
FPT_ITA.1	O.INTERFACE

Requirements	Objectives
FPT_RCV.2	O.SELF_PROTECT, OE.BACKUP
FPT_RVM.1	O.SELF_PROTECT, OE.BACKUP
FPT_SEP.1	O.SELF_PROTECT
FPT_STM.1	O.AUDIT, OE.INSTALL
FPT_TDC.1	O.INTERFACE
FPT_TST.1	O.DETECT, O.SELF_PROTECT, OE.BACKUP
FTA_LSA.1	O.POLICY, OE.ADMIN
FTA_MCS.1	O.POLICY, OE.ADMIN
FTA_SSL.3	O.I&A, O.POLICY, O.SELF_PROTECT
FTA_TSE.1	O.ACCESS_ADMIN, O.POLICY
FTP_TRP.1	O.INTERFACE
ITR_AUD_REV	OE.AUDITLOG, OE.TRAIN
NITR_ADMIN_TRAIN	OE.INSTALL, OE.TRAIN
NITR_PHYSICAL	OE.PHYSICAL

6.6 Explicit Requirements Rationale

To be consistent with the rest of the Mobile Code Enclave, the explicit requirements rationale is located in Section 6.3 on page 41.

Appendix A — Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

References

Common Criteria Implementation Board, *Common Criteria for Information technology Security Evaluation*, CCIB-98-026, Version 2.2, May 1998

National Information System Security (INFOSEC) Glossary. NSTISSI No. 4009, January 1999 (Revision 1)

Department of Defense (DoD) Mobile Code Technology Policy and Guidance, (DRAFT) 21 June 2000.

Definition and Risk Categorization for Mobile Code Formats, Version 1.0, 12 November 2000